Date

ROUTING AND TRANSMITTAL SLIP

TO: (Name, office symbol, room number, building, Agency/Post)	Initials	Date
1. EXO	GD	10 May 83
2. DD	[illegible]	10 May 83
3. D	[illegible]	11.5.83
4.		
5.		

	Action		File		Note and Return
	Approval		For Clearance		Per Conversation
	As Requested		For Correction		Prepare Reply
	Circulate		For Your Information		See Me
	Comment		Investigate		Signature
	Coordination		Justify		

REMARKS

DO NOT use this form as a RECORD of approvals, concurrences, disposals, clearances, and similar actions

FROM: (Name, org. symbol, Agency/Post)	Room No.—Bldg.
	Phone No.

5041-102

OPTIONAL FORM 41 (Rev. 7-76)
Prescribed by GSA
FPMR (41 CFR) 101-11.206

☆U.S.GPO:1978-0-261-647 3354

ODP-83-675
May 10, 1983

MEMORANDUM FOR: Chief, Information Systems Security Group,
Office of Security, DDA

Chief, Systems Group,
Information Management Staff, DDO

STAT FROM: [redacted]
CIA Representative,
CIRS Management Group

SUBJECT: Proposed Work Statement for Support of CIRS Security Working Group

REFERENCE: A. Task III, Work Statement for Support of CIRS Computer Security Working Group, dated 4 May 1983

B. Proposed Tasking Statement for CIRS Security Working Group, dated 12 January 1983

1. Attached you will find copies of references A and B for your review. During the CIRS Management Group (CMG) meeting of 5 May 1983, STAT [redacted] STAT Chairman, CMG, submitted reference A for approval. I indicated that I was not in a position to approve this statement without consultation with the appropriate Agency components. In addition, I felt that reference B should be more general in nature.

2. I withheld approval of reference A, pending further Agency review and coordination, for the following reasons:

- o The word "Computer" should be deleted from the title since the name of the group is properly the "CIRS Security Working Group". The intent here is not to limit working group purview to computer security issues but rather to include all aspects

which may bear on CIRS security.

- Without concurrence from the responsible Agency components, I could not approve a proposal permitting the CIRS support contractor, MITRE Corp., access to Agency resources for the purpose of evaluating the security policies and procedures of CIA computer systems and networks. The proposal calls for the contractor to "evaluate the security features ... including software, hardware, procedures, physical, personnel clearance procedures, TEMPEST, and COMSEC.";

- Without concurrence from the responsible Agency components, I could not approve a proposal permitting the CIRS support contractor to review and evaluate the RECON GUARD project; and

- The proposal should be changed to call for the production of a CIRS Requirements/Policy Document rather than a security plan; we should determine where we want to go before we draw up a plan detailing how to get there.

3. I also feel that reference B, which I have not approved, is too specific. The tasking statement should be presented in terms of a general objective, leaving the details of how to accomplish it up to the Security Working Group.

4. It is important that we proceed in concert on these issues and that the CIRS Security Working Group (CSWG) have a broad tasking statement to allow it to properly develop a CIRS Security Requirements/Policy Document. I look to the CSWG to develop such a document and the CIA CSWG representatives to formulate and present the Agency position on this vital issue. Accordingly, I will propose to the CMG that:

- The word "Computer" in the title of reference A be deleted;

- The specifics of reference A be left up to the members of the CSWG; and

- Reference B be reworded to provide a broad tasking statement to include the production of a CIRS Security Requirements/Policy Document. This document will serve as the basis for the

development of satisfactory CIRS security controls and procedures.

5. Should you feel that the positions on reference A and B, as presented above, should be altered or have any questions or comments regarding CIRS security for which I might be of assistance please do not hesitate to contact me. I can be reached on

STAT
STAT
STAT

cc:

D/ODP
C/MS/ODP
C/ISG/OCR/DDI
C/INT/PCS/DDO
C/PATG/ORD/DDS&T

Att: a/s

master

1230

4 May 1983

Task III

Work Statement for Support of CIRS
Computer Security Working Group

The contractor will work in support of the government sponsored CIRS Computer Security Working Group to evaluate the security policies and procedures of the five computer systems (i.e., NSA SOLIS/WINDMILL, FTD CIRC, CIA and DIA SAFE, and new NPIC NDS) and two networks (i.e., COINS II and DODIIS) that will be used in accordance with the CIRS plan. Government representatives who are responsible for the security of the five systems and two networks will brief and provide documentation to the contractor. Meetings between the contractor and the government members will be arranged by the CIRS coordinator. The contractor will evaluate the security features of each of these components in areas including software, hardware, procedures, physical, personnel clearance procedures, TEMPEST, and COMSEC. The contractor will use the evaluation criteria established by the DOD Computer Security Evaluation Center and other appropriate evaluation methodologies to provide an overall assessment of each of the components. The CIRS plan calls for these systems to operate in a "compartmented mode" of operations by 1990. Existing security procedures and any proposed new procedures should be evaluated or developed in accordance with this objective. The following substasks are included in this task:

Subtasks I - Documentation Review and Evaluation Criteria Development

The contractor will review and be familiar with current and proposed versions of DCID 1/16, DOD Directive 5200.28, DIA Manual 50-4, DOD Computer Security Evaluation Center Evaluation Criteria, DODIIS DIN VI Criteria, and other pertinent documentation. The contractor will develop evaluation criteria for his efforts for review and approval by the government members of the working group. This subtask which will be documented in the form of a memorandum for the record will be completed within two weeks of task initiation and revised as necessary throughout the performance of the task.

Subtask II - Review and Evaluate Security Features of Each of the Component Systems

The contractor will review the security features of each of the components and document the features of each of these systems in the form of memoranda for the record. Briefings and documentation will be provided for the contractor as necessary and demonstrations of the features will be provided if possible. The contractor will consider the security features such as password protection, host control access procedures, and remote user identification in his evaluation. The contractor will focus on the security features used by each of the systems to protect ORCON, EXDIS, LIMDIS, and eventually the possible inclusion of "G" materials.

Subtask III - Review and Evaluate RECON Guard Approach and Other New Features

The contractor will review the current progress of the RECON GUARD approach, the DIA fingerprint matrix identifier, BLACKER, DIN VI, and other new security facilities to assess their possible use in the overall CIRS effort. Such an assessment will include a technical risk assessment as well as a cost evaluation for the use of these features. These efforts will be documented in the form of memoranda within the third month of the contractural effort.

Subtask IV - Develop Proposed Security Standards for Overall CIRS Operations

The contractor shall use all the previous analyses to develop draft security standards for processing under the CIRS plan. These draft security standards will be documented in a draft CIRS Security Plan that will include the identification of enhancements which must be made to each of the CIRS components in order to achieve these standards. This initial plan will also include resource estimates and identify milestone dates for the enhancement of each of the CIRS components. This initial CIRS Security Plan shall be completed within seven months from the initiation of this task. Upon review and possible modification by the government, this plan wil be revised at a future date under a separate task effort.

ILLEGIB

Length of Task: Seven months from initiation of the task.

Resources: Approximately 5.0 man-months of effort.

Deliverables:

a. Subtask I - Memorandum for the record providing evaluation criteria for review and approval by working group.

b. Subtask II - Memoranda on the evaluation of each of the component systems.

c. Subtask III - Memoranda on RECON GUARD and other specialized security features.

d. Subtask IV - Final written report and briefing which summarize all previous efforts and presents the contractor's proposed initial CIRS Security Plan which will be reviewed and approved by the CIRS Computer Security Working Group and the full IHC.

e. Monthly status reports.

Travel Requirement:

a. Local travel.

b. One two-day trip to Dayton, Ohio, to visit the FTD facility.

Clearance Required:

a. Personnel

- o Agency TS/SI/TK/GAMMA with CIA polygraph for professionals working directly on effort.
- o Agency TS/SI/TK for admin personnel involved with the effort.

b. Contractor Facility

- o Facility clearance for storage of TS/SI/TK materials.

Attachment 5

12 January 1983

PROPOSED TASKING STATEMENT FOR CIRS SECURITY WORKING GROUP

The CIRS Security Working Group will include agency/component representatives who are responsible for the security policies and procedures of computer systems and networks to be used in accordance with the CIRS plan. This working group will be supported by contractor/consultants and be tasked to do the following:

- Review current security procedures of existing automated systems/data communications networks which will provide processing services under the CIRS plan highlighting variations in hardware, software, and procedural approaches (e.g., password protection, host control access procedures, terminal identifiers).

- Review future security procedures to be incorporated in systems/networks such as SAFE, COINS, and the DODIIS DIN VI model as well as any future changes to security in current processors.

- Concentrate on security features and procedures for the protection of ORCON, "G" materials, EXDIS, and LIMDIS identifying how current systems are controlling access and how CIA and DIA SAFE will handle these materials in the future.

- Review the status and future potential of the RECON GUARD approach and assess its capability to be used as a feature for some or all of CIRS processors.

- Assisted by the IHC staff and contractor/consultants, develop a preliminary and final security plan for the overall CIRS effort incorporating minimum security features that each host and network must maintain in order to provide the specified services under the CIRS plan. Identify by system/network what enhancements must be made by milestone date in order to process the "generally available data" as well as the more highly sensitive material (i.e., "G" material).

- Assist in the development, review and approval of a preliminary security plan by 1 September 1983 to be briefed to the IHC and updated on a quarterly basis.